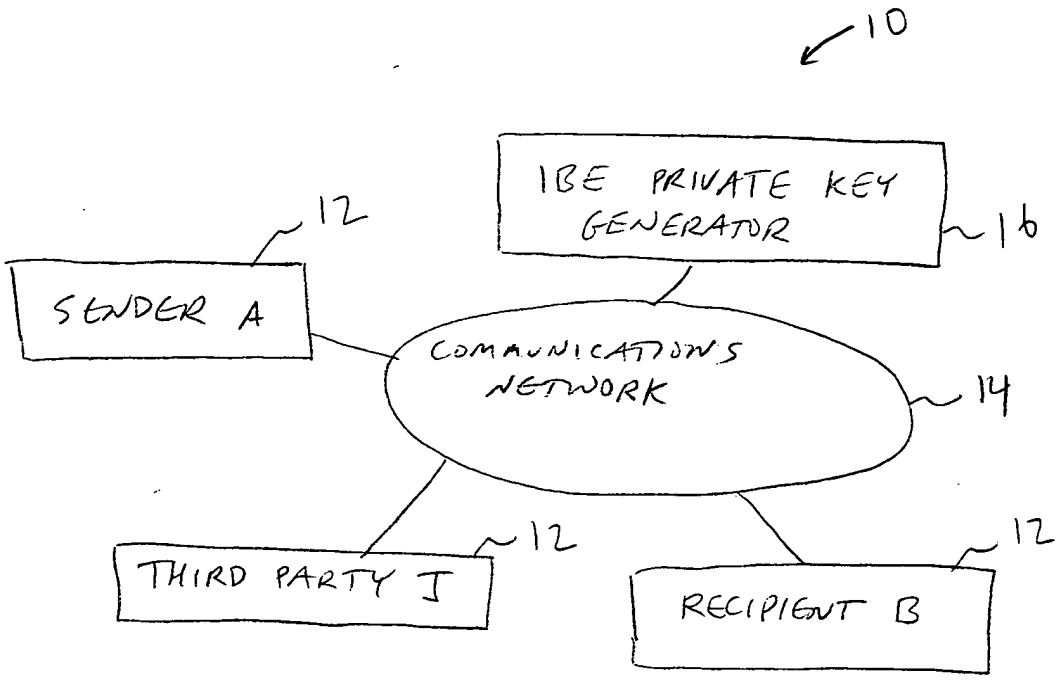
10
IBE PRIVATE KEY GENERATOR
16
12
SENDER A
COMMUNICATIONS NETWORK
14
12
THIRD PARTY I
12
RECIPIENT B

FIG. 1

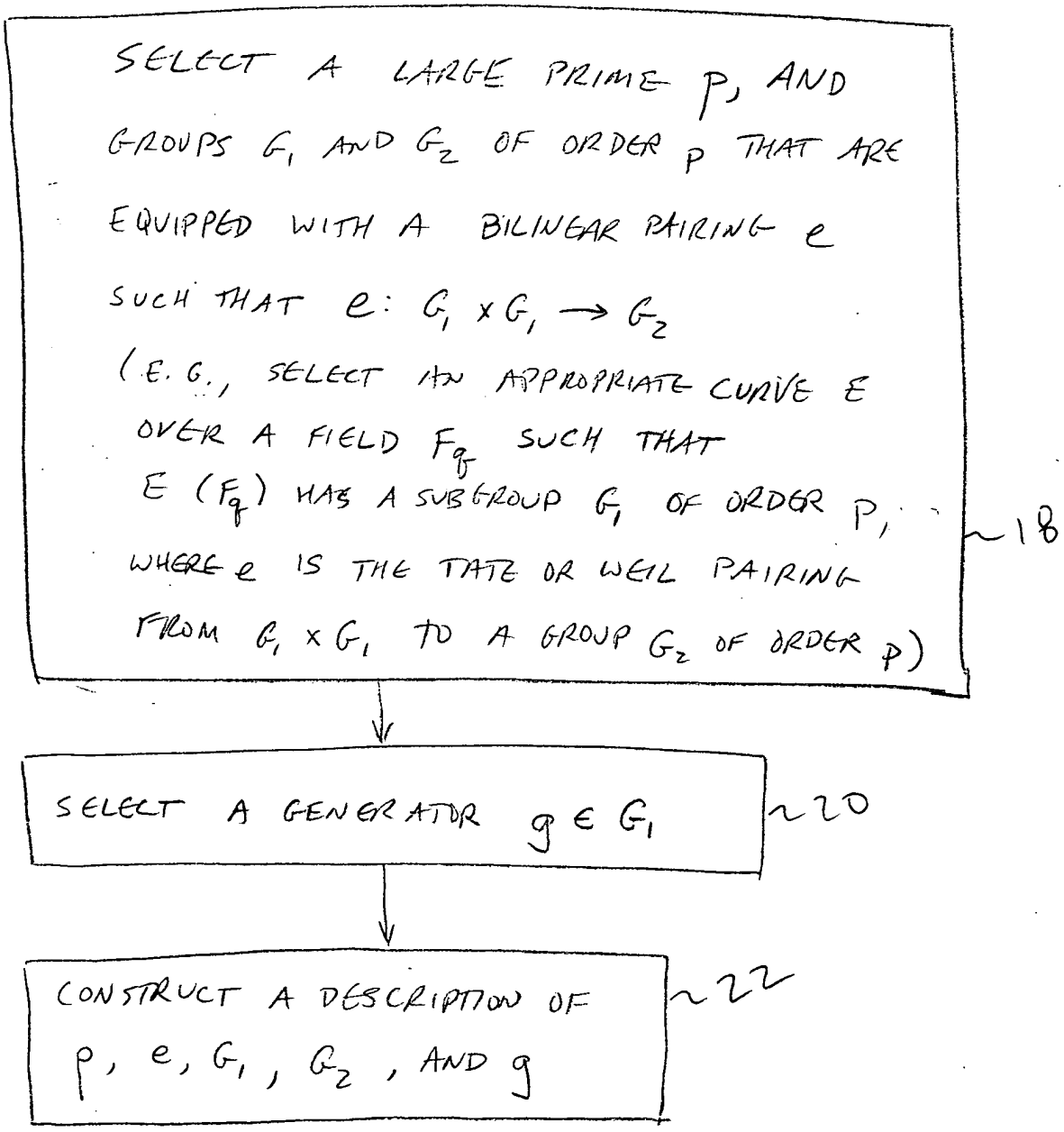
SELECT A LARGE PRIME p, AND GROUPS G_1 AND G_2 OF ORDER p THAT ARE EQUIPPED WITH A BILINEAR PAIRING e SUCH THAT $e: G_1 \times G_1 \rightarrow G_2$ (E.G., SELECT AN APPROPRIATE CURVE E OVER A FIELD F_q SUCH THAT $E(F_q)$ HAS A SUBGROUP G_1 OF ORDER p, WHERE e IS THE TATE OR WEIL PAIRING FROM $G_1 \times G_1$ TO A GROUP G_2 OF ORDER p)
18
SELECT A GENERATOR $g \in G_1$
20
CONSTRUCT A DESCRIPTION OF p, e, G_1, G_2, AND g
22

FIG. 2

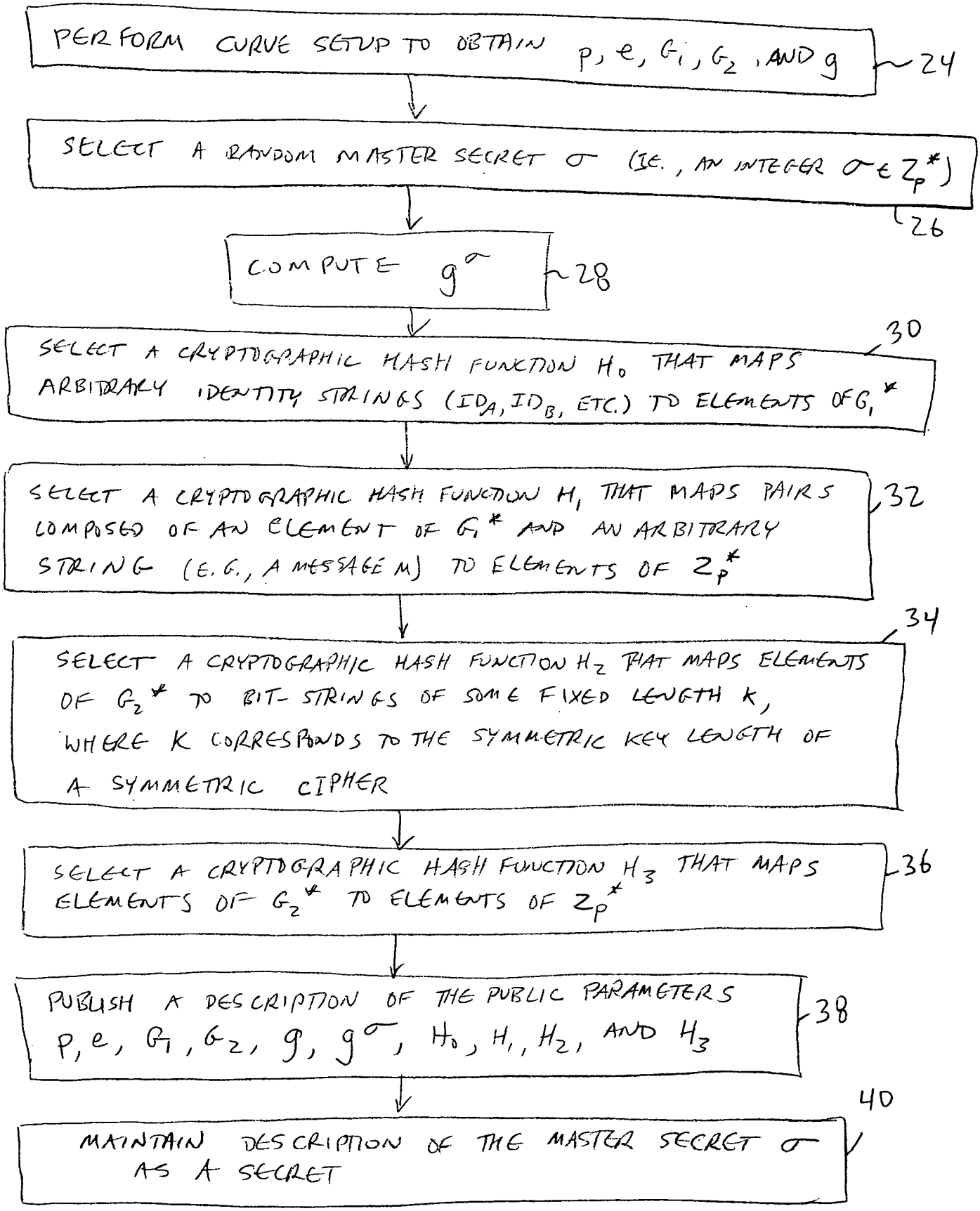
PERFORM CURVE SETUP TO OBTAIN p, e, G_1, G_2, AND g
24
SELECT A RANDOM MASTER SECRET σ (IE., AN INTEGER $\sigma \in Z_p^*$)
26
COMPUTE g^σ
28
SELECT A CRYPTOGRAPHIC HASH FUNCTION H_0 THAT MAPS ARBITRARY IDENTITY STRINGS (ID_A, ID_B, ETC.) TO ELEMENTS OF G_1^*
30
SELECT A CRYPTOGRAPHIC HASH FUNCTION H_1 THAT MAPS PAIRS COMPOSED OF AN ELEMENT OF G_1^* AND AN ARBITRARY STRING (E.G., A MESSAGE M) TO ELEMENTS OF Z_p^*
32
SELECT A CRYPTOGRAPHIC HASH FUNCTION H_2 THAT MAPS ELEMENTS OF G_2^* TO BIT-STRINGS OF SOME FIXED LENGTH K, WHERE K CORRESPONDS TO THE SYMMETRIC KEY LENGTH OF A SYMMETRIC CIPHER
34
SELECT A CRYPTOGRAPHIC HASH FUNCTION H_3 THAT MAPS ELEMENTS OF G_2^* TO ELEMENTS OF Z_p^*
36
PUBLISH A DESCRIPTION OF THE PUBLIC PARAMETERS $p, e, G_1, G_2, g, g^\sigma, H_0, H_1, H_2$, AND H_3
38
MAINTAIN DESCRIPTION OF THE MASTER SECRET σ AS A SECRET
40

FIG. 3

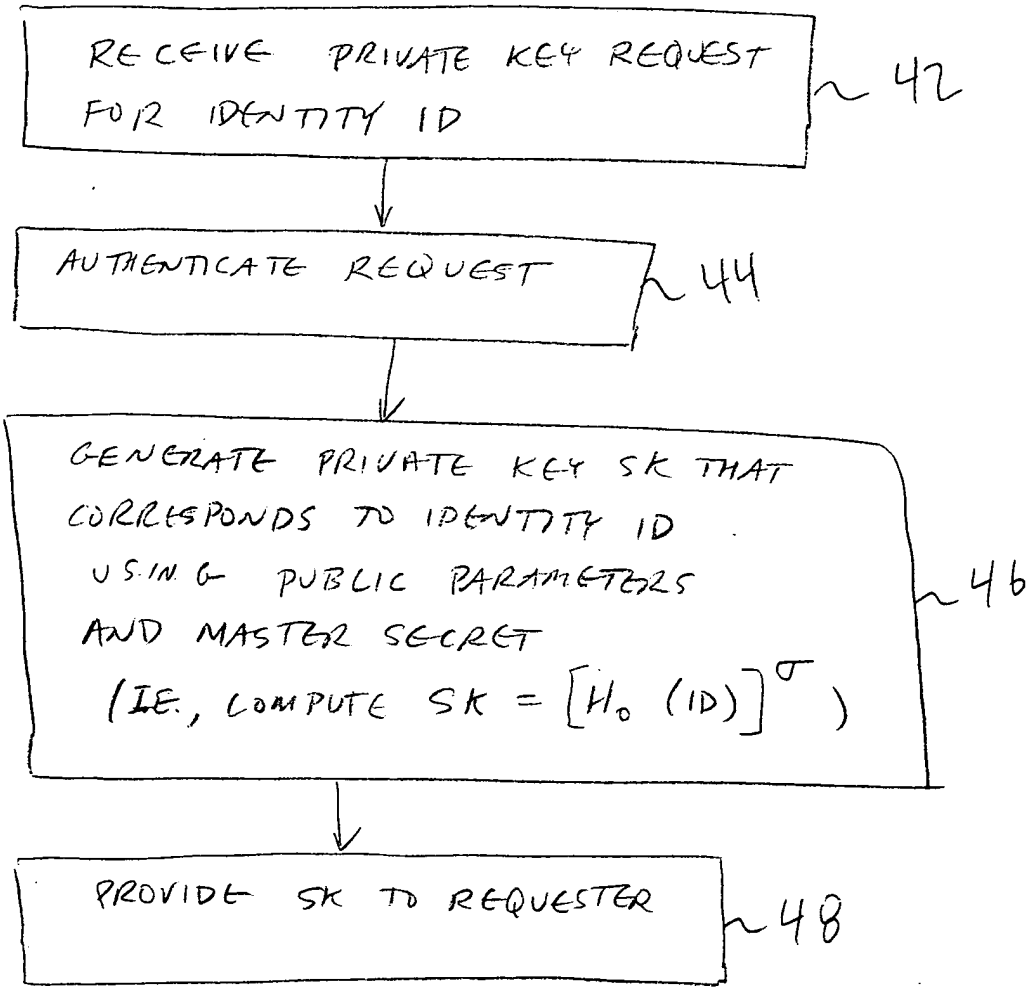
RECEIVE PRIVATE KEY REQUEST FOR IDENTITY ID
42
AUTHENTICATE REQUEST
44
GENERATE PRIVATE KEY SK THAT CORRESPONDS TO IDENTITY ID USING PUBLIC PARAMETERS AND MASTER SECRET
(IE., COMPUTE $SK = [H_0(ID)]^{\sigma}$)
46
PROVIDE SK TO REQUESTER
48

FIG. 4

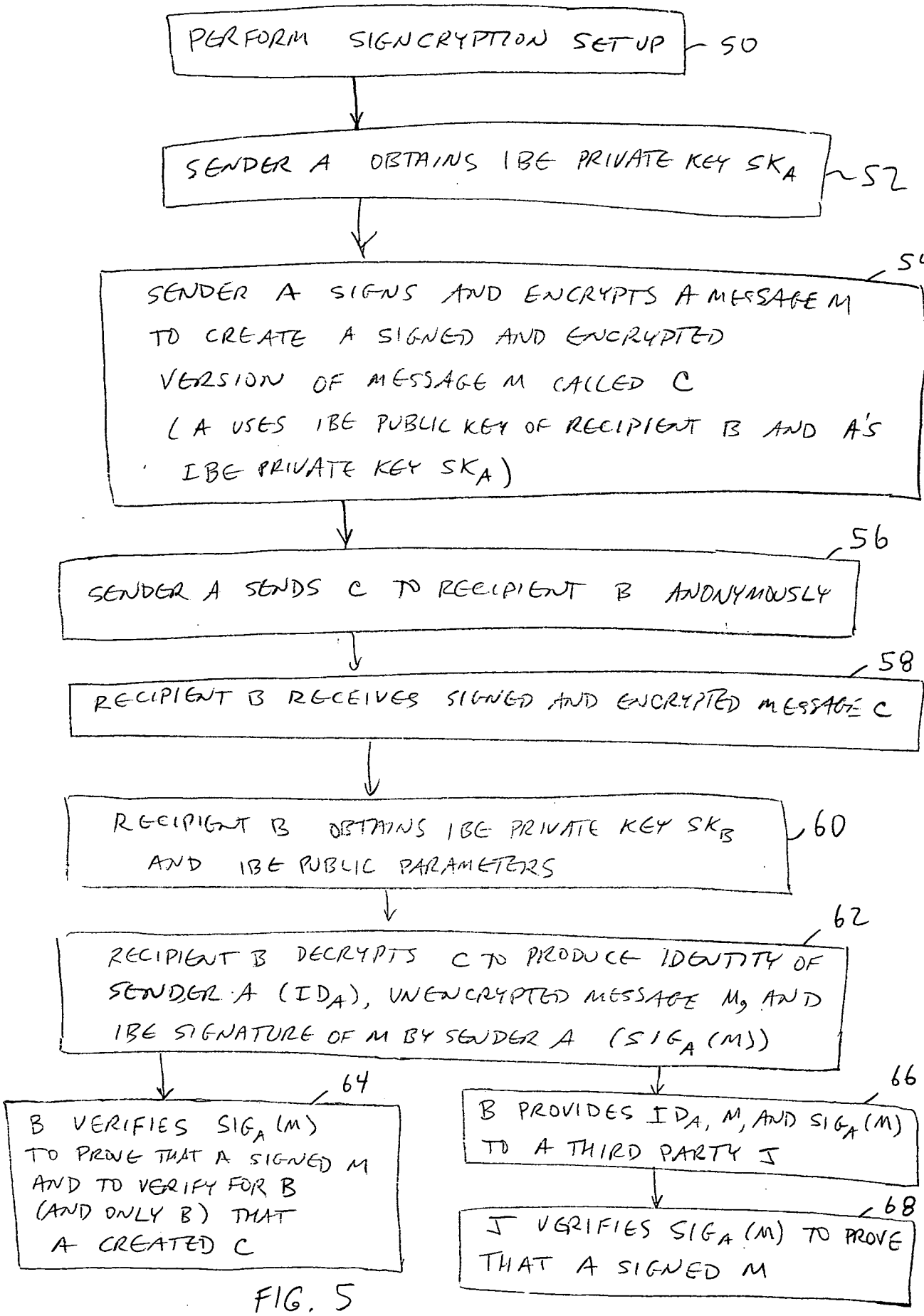
PERFORM SIGNCRYPTION SETUP
50
SENDER A OBTAINS IBE PRIVATE KEY SK_A
52
54
SENDER A SIGNS AND ENCRYPTS A MESSAGE M TO CREATE A SIGNED AND ENCRYPTED VERSION OF MESSAGE M CALLED C (A USES IBE PUBLIC KEY OF RECIPIENT B AND A'S IBE PRIVATE KEY SK_A)
56
SENDER A SENDS C TO RECIPIENT B ANONYMOUSLY
58
RECIPIENT B RECEIVES SIGNED AND ENCRYPTED MESSAGE C
RECIPIENT B OBTAINS IBE PRIVATE KEY SK_B AND IBE PUBLIC PARAMETERS
60
62
RECIPIENT B DECRYPTS C TO PRODUCE IDENTITY OF SENDER A (ID_A), UNENCRYPTED MESSAGE M_0 AND IBE SIGNATURE OF M BY SENDER A ($SIG_A(M)$)
64
B VERIFIES $SIG_A(M)$ TO PROVE THAT A SIGNED M AND TO VERIFY FOR B (AND ONLY B) THAT A CREATED C
66
B PROVIDES ID_A, M, AND $SIG_A(M)$ TO A THIRD PARTY J
68
J VERIFIES $SIG_A(M)$ TO PROVE THAT A SIGNED M

FIG. 5

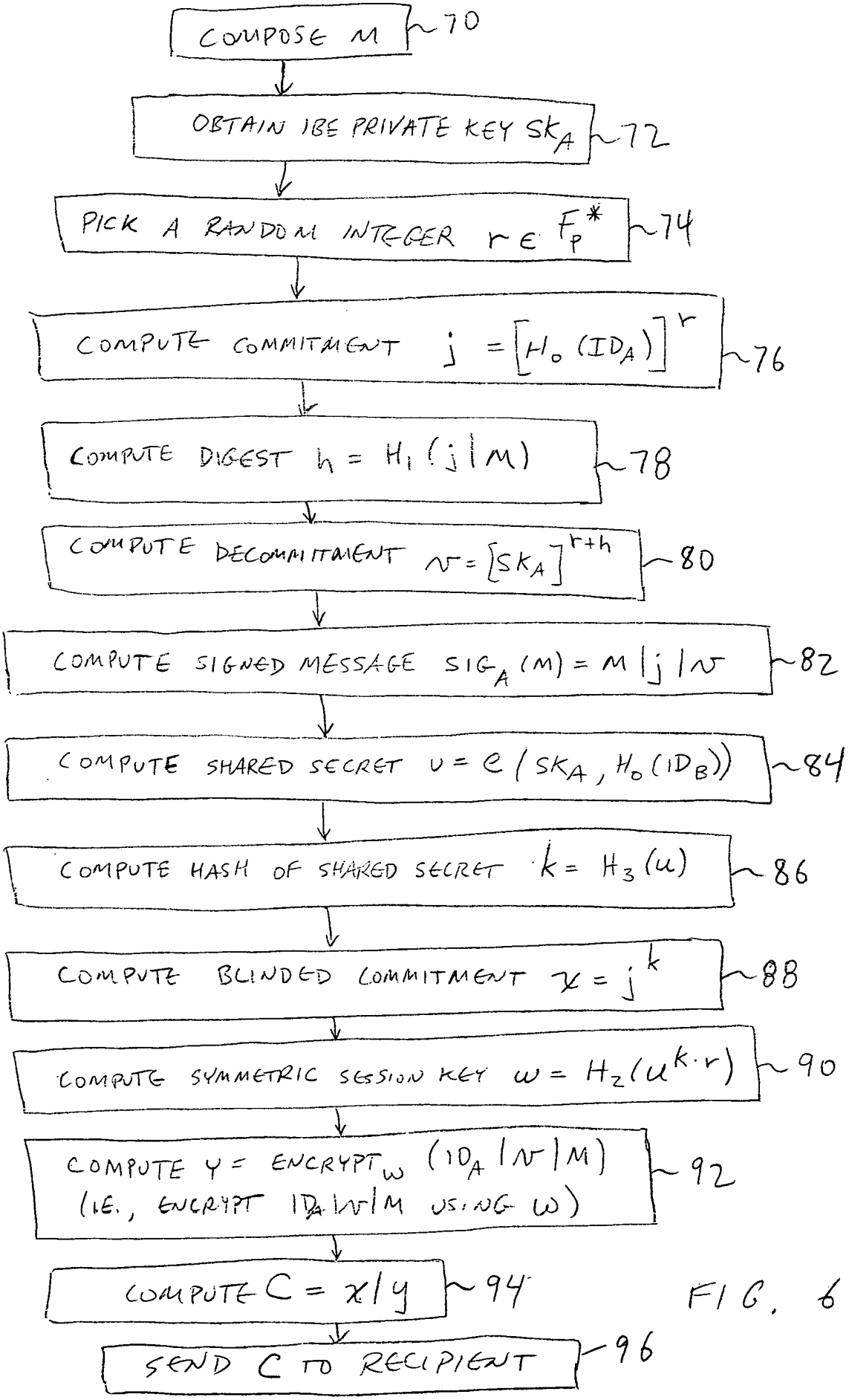
COMPOSE M
70
OBTAIN IBE PRIVATE KEY SK_A
72
PICK A RANDOM INTEGER $r \in F_p^*$
74
COMPUTE COMMITMENT $j = [H_0(ID_A)]^r$
76
COMPUTE DIGEST $h = H_1(j|M)$
78
COMPUTE DECOMMITMENT $v = [SK_A]^{r+h}$
80
COMPUTE SIGNED MESSAGE $SIG_A(M) = M|j|v$
82
COMPUTE SHARED SECRET $u = e(SK_A, H_0(ID_B))$
84
COMPUTE HASH OF SHARED SECRET $k = H_3(u)$
86
COMPUTE BLINDED COMMITMENT $x = j^k$
88
COMPUTE SYMMETRIC SESSION KEY $w = H_2(u^{k \cdot r})$
90
COMPUTE $Y = ENCRYPT_w(ID_A|v|M)$
(I.E., ENCRYPT $ID_A|v|M$ USING w)
92
COMPUTE $C = x|y$
94
SEND C TO RECIPIENT
96

FIG. 6

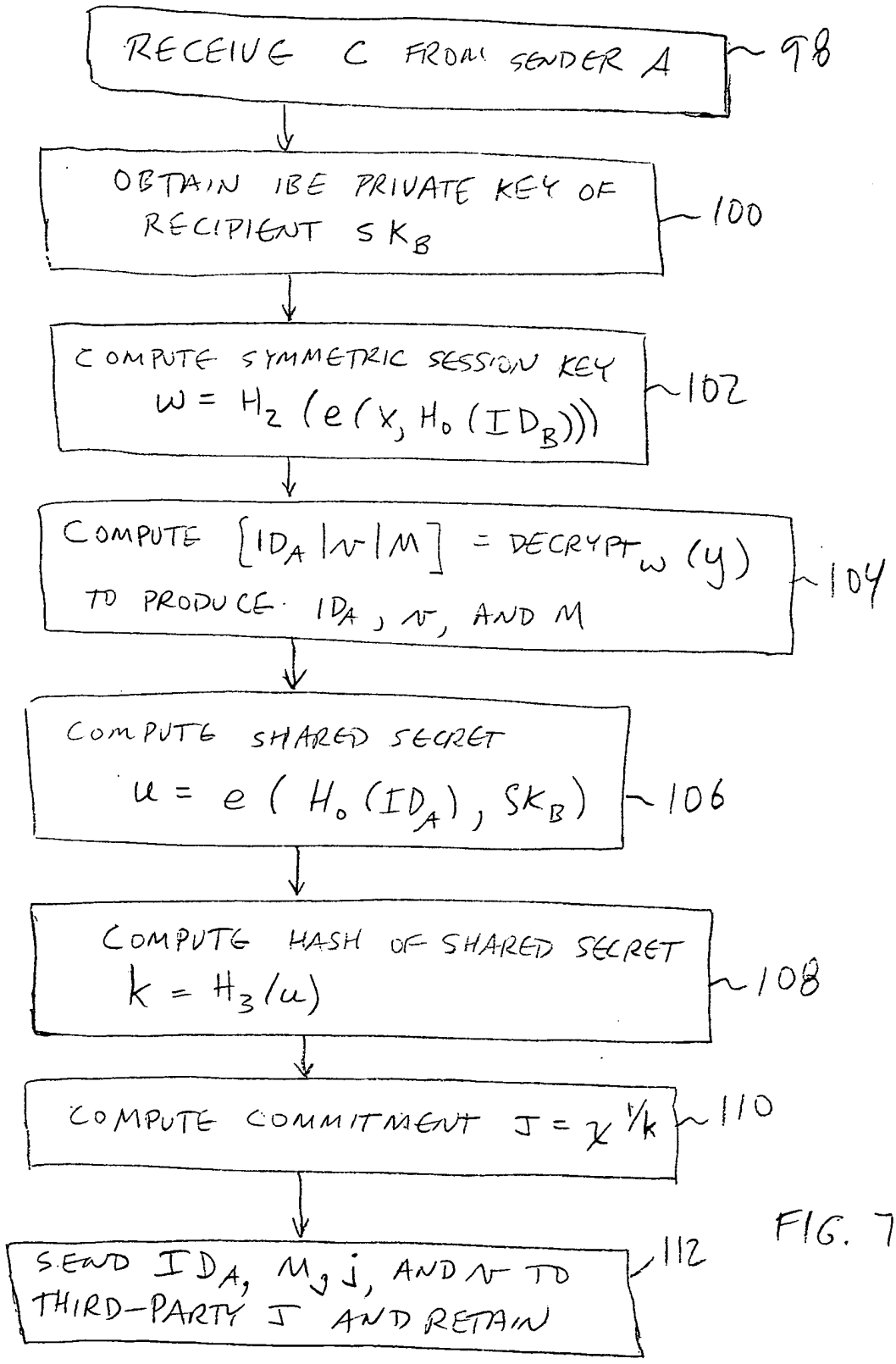
RECEIVE C FROM SENDER A
98
OBTAIN IBE PRIVATE KEY OF RECIPIENT SK_B
100
COMPUTE SYMMETRIC SESSION KEY $w = H_2(e(x, H_0(ID_B)))$
102
COMPUTE $[ID_A | r | M] = \text{DECRYPT}_w(y)$ TO PRODUCE ID_A, r, AND M
104
COMPUTE SHARED SECRET $u = e(H_0(ID_A), SK_B)$
106
COMPUTE HASH OF SHARED SECRET $k = H_3(u)$
108
COMPUTE COMMITMENT $J = \chi^{1/k}$
110
SEND ID_A, M, j, AND r TO THIRD-PARTY J AND RETAIN
112

FIG. 7

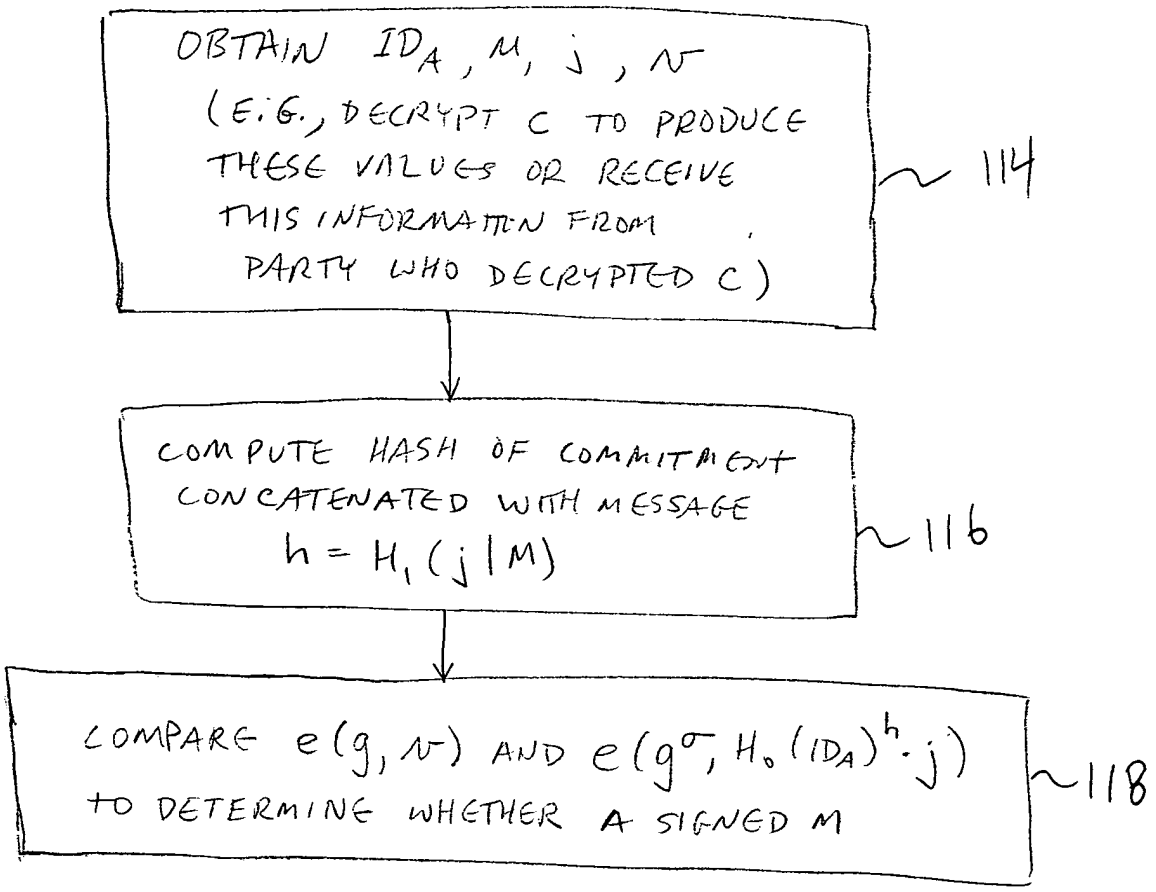
OBTAIN ID_A, M, j, σ
(E.G., DECRYPT C TO PRODUCE THESE VALUES OR RECEIVE THIS INFORMATION FROM PARTY WHO DECRYPTED C)
114
COMPUTE HASH OF COMMITMENT CONCATENATED WITH MESSAGE
$h = H_1(j|M)$
116
COMPARE $e(g, \sigma)$ AND $e(g^{\sigma}, H_0(ID_A)^h \cdot j)$ TO DETERMINE WHETHER A SIGNED M
118

FIG. 8